475 Anton Boulevard
Costa Mesa, CA 92626
www.experian.com

January 28, 2011

Via Email: privacynoi2010@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

Re: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework – Comment, Docket No. 101214614-0614-01

Dear Internet Policy Task Force:

Experian appreciates this opportunity to provide comments on the Department of Commerce Internet Policy Task Force's ("Department") report titled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* ("Commerce Report").[1]

As steward of some of the leading consumer information databases—all of which are regulated by federal and state law and industry self-regulatory standards—Experian has unique insight into how third-party data is collected, and how it is used by commercial, non-profit, and government entities. In addition, Experian also provides many services directly to consumers, including leading products to help provide consumer financial literacy and education directly to millions of Americans.

We believe robust industry self-regulation coupled with existing sectoral privacy laws and enforcement of unfair and deceptive trade practices continues to be the most effective way to balance consumer privacy interests with business ingenuity. Experian is committed to ensuring that a self-regulatory framework succeeds that fosters consumer trust, spurs innovation, and secures consumer data. We urge the Department to support the self-regulatory initiatives that are currently underway and to encourage businesses to participate in such efforts.

I. Background on Experian Products and Services.

Experian is a leading global information services company, providing analytical and marketing services to organizations and consumers to help manage the risk and reward of commercial and financial decisions. Experian is well known in the United States as one of the three national crediting reporting agencies, but credit reporting is only one aspect of our business. For more than fifty years, Experian has compiled consumer data and used the information to help facilitate direct marketing, primarily through the U.S. Mail. Over these years, there have been many changes in technology and the manner in which organizations

[1] Department of Commerce Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (December 2010) (hereinafter "Commerce Report").

communicate and advertise to their current and prospective members or customers. Experian uses its compiled databases to facilitate multi-channel marketing and advertising through the mail, telephone, and email. The emergence of Experian's Digital Advertising Services brings the same compiled marketing information and direct marketing principles to television, online, and mobile advertising.

Experian serves large and small corporations and non-profit organizations around the world, and in doing so, has adopted five global information values that guide our use of marketing data. These values—balance, accuracy, security, integrity, and communication—align with the Fair Information Practice and Principles ("FIPPs") embraced by the Department, the Organization for Economic Cooperation & Development, the European Union, and the Asia-Pacific Economic Corridor. These information values form the foundation of our belief that information use must benefit both businesses and individuals, while simultaneously meeting the privacy expectations of consumers.

Because Experian has operations in 90 countries, we must apply these information values according to the laws, customs, and consumer expectations of the nations and regions in which it operates and/or serves customers. In turn, information policies, built upon our values, more specifically define how information may be used. For example, our privacy and compliance team works closely with Experian's business units to perform a proactive risk assessment prior to all data sourcing and product development launches. This self-regulatory audit incorporates subject matter experts from every relevant functional area of the company, including product development, technology, legal, compliance, information security, risk management, and data acquisition.

In addition, Experian has demonstrated a commitment to providing consumers notice, choice, and education about the use of personal information through our collateral materials and information available on each of our public-facing websites. We also allow consumers to easily exercise choice with respect to the use of their personal information and provide our clients with the ability to utilize available suppression files.

II. Third-Party Sharing of Data Provides Significant Benefits to Consumers and Businesses.

The collection and sharing of third-party consumer data, which is at the heart of Experian's consumer databases, provides numerous significant benefits to consumers and businesses. Our market research and analysis services help businesses identify the common characteristics of their customers, which allows them to plan better media campaigns, determine the best retail or branch site locations, develop new product offerings, tailor their editorial content, and ensure adequate product inventory. The result is lower prices, enhanced competition, and increased consumer convenience.

Third-party data also facilitates the relevancy of first-party marketing efforts, especially for small businesses and start-ups, which rely heavily on marketing to prospective customers. Even large first-party marketers with extensive customer databases depend on third-party data to provide better services and relevant marketing offers to existing customers. Marketers cannot rely solely on their own transactional and experience data to effectively make offers that are

tailored to specific individual or household preferences. This reduces the total number of advertising impressions that are produced, thus reducing the delivery of irrelevant advertising, which benefits consumers.

We further believe that the U.S. approach for protecting personal data—built on strong sectoral laws and voluntary enforceable codes of conduct that have been in place for decades—is instrumental to the success and growth of the U.S. economy. The exchange of information among affiliated organizations, third parties, and consumers fuels innovation and product development, which in turn drives the United States economy. Breakthroughs in information technology that enable, for example, the ubiquity of social networking and e-commerce, simply would not have been possible without the collection and sharing of data. The existing approach to data security and consumer privacy is key to ensuring U.S. businesses continue to lead the world in the development of cutting-edge and transformative products and services. Because of this, and as addressed further below, Experian would urge the Department to present and support the existing U.S. framework as the best model for other nations to adopt in any effort to reach a global, harmonized regime.

Any privacy framework should carefully balance restrictions on the collection and sharing of third-party information with the significant benefits that these uses of information provide to consumers, businesses, and the economy at large. Unlike static laws and regulatory regimes that cannot keep pace with rapidly developing technologies, we believe that self-regulatory systems are inherently adaptive and thus best suited to respond to new, emerging technologies and consumer needs while maintaining the competitive edge of the United States in the global economy.

III. A FIPPs-Based Framework Could Serve as a Useful Tool for Companies to Evaluate Their Practices, But Not as a Legislative or Regulatory Framework.

The Department has recommended the development of a full set of FIPPs as a foundation for commercial data privacy policy enacted either by industry, the Executive Branch, or Congress. While Experian believes that a FIPPs-based framework could be used by companies to evaluate their privacy and data security practices at various stages of the development of their products and services, we do not believe a new legal regime governing consumer privacy is needed. Ultimately, consumers are adequately protected by the existing system of U.S. sectoral laws (federal and state), multiple regulations promulgated and enforced there under, robust yet flexible self-regulatory codes of conduct, and strong enforcement by the Federal Trade Commission of unfair and deceptive trade practices.

There is therefore not a demonstrated need for—nor any evidence supplied by the Department in its report to justify—adopting new legal requirements to protect consumer privacy given the established multi-layered system our nation has developed over the past forty years. Financial and health information is already afforded substantial privacy protections under existing laws, including the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, the Fair Billing Act, the Health Insurance Portability and Accountability Act, and the Wall Street Reform and Consumer Protection Act. Similarly, data related to children is subject to strong legal protections under the Children's Online Privacy Protection Act. Moreover, data collected

for marketing purposes has been effectively regulated by standards promulgated by industry groups, such as the Direct Marketing Association ("DMA"), for over forty years.

Second, the codification of a FIPPs-based framework through legislation or government-driven regulation that broadly applied to all data practices would inevitably produce a set of inflexible top-down prescriptions. This outcome would unnecessarily hamper the business community's ability to drive innovation and address rapidly evolving consumer preferences. We agree with the Department that a comprehensive baseline set of FIPPs must maintain the flexibility for each industry sector to develop tailored implementation plans and allow companies to direct resources to the principles that matter most for protecting privacy in a particular context in order to succeed.[2] However, we do not believe any government law or regulation, however carefully drafted, could retain those principles and simultaneously provide meaningful, enforceable guidance over time given the ever-developing and highly dynamic nature of business operations in the information age.

Experian strongly believes self-regulation is the most effective way to regulate commercial data used for marketing purposes. Such self-regulatory codes of conduct are most effective when developed by the businesses to which the standards would apply, and not by government agencies or other groups. For over forty years, industry has taken the lead in developing and enforcing responsible codes of conduct. The guidelines and standards of the DMA, for example, provide individuals and organizations involved in direct marketing with a comprehensive set of principles that cover all marketing practices, including the collection, use, and maintenance of marketing data.[3] To enforce these guidelines, the DMA has established a committee which examines promotions and practices of members and nonmembers that may violate DMA's guidelines. The committee successfully works with individuals and companies to gain voluntary cooperation in adhering to the guidelines and to adopt good business practices for direct marketers. The DMA Guidelines for Ethical Business Practice have been applied to hundreds of direct marketing cases concerning deception, unfair business practices, personal information protection, and other ethics issues. In the last two years, the business community has demonstrated its deep commitment to effective self-regulation online. In July 2009, a coalition of industry organizations released the *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles") and then launched a self-regulatory program covering these practices in early fall 2010.[4] These successful initiatives, which serve as models for further self-regulatory efforts, are a testament to the industry's dedication to the principles of self-regulation and its ability to deliver.

We agree with the Department that the federal government has a significant role to play in harmonizing data security standards across state lines and international borders. That is why we support the adoption of a national standard for security breach notification that applies only to data that constitutes sensitive personally identifiable information. By simplifying business

---

[2] Commerce Report at 25.

[3] Direct Marketing Association, *Guidelines for Ethical Business Practice* (revised January 2010), *available at,* http://www.dmaresponsibility.org/Guidelines/.

[4] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009)*, available at,* http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

compliance processes and reducing costs, the adoption of a single, preemptive standard would increase and strengthen compliance.

IV. The Department Should Facilitate the Development of Global Interoperability and Harmony of Data Security Standards Across Countries.

Experian operates in more than 90 countries around the world and thus faces the challenges caused by the multiplicity of foreign data protection rules and regulations on a daily basis. We support the Department's call for the U.S. government to increase its efforts to develop a framework for mutual recognition of international data security standards. We do not, however, believe that the goal of such a framework should be a "one-size-fits-all" universal privacy standard. A country's cultural norms define the level and type of privacy rights expected by its citizens. A global standard of privacy detached from U.S. privacy norms and consumer preferences should not be imposed on American consumers. We instead urge the Department to advocate for a global framework that that recognizes each country's unique approach to privacy.

While we believe privacy standards are local, information security should be global. Entities that maintain personal data should meet international standards of data security. Data should be able to be processed anywhere in the world, so long as appropriate data security standards are in place and the use of such data does not violate the privacy laws of the country in which the consumer resides. Better reconciliation of global security standards, coupled with adherence to country-specific privacy rights, would quell concerns about international transfers of information or the use of cloud computing. As such, we encourage the Department to lead international efforts to develop a framework that harmonizes data security standards across countries.

* * *

Experian thanks you for the opportunity to engage in dialogue with the Commission on these important matters. Should you have any questions, please do not hesitate to contact me at (202) 682-4613.

Sincerely,

Tony Hadley
Senior Vice President
Government Affairs